Nationaal Cyber Security Centrum
Ministerie van Veiligheid en Justitie

NCSC Maandmonitor

Januari 2016

TLP: GROEN

versie 1.0 | 1 februari 2016

A

[redacted]

Cyberaanval leidt mogelijk tot stroomuitval in Oekraïne

Diverse media rapporteerden dat eind vorig jaar gedurende 6 uur een stroomstoring is opgetreden in een aantal regio's in Oekraïne. [1][2] De storing zou zijn veroorzaakt door cyberaanvallen op de ICS-infrastructuur van de stroomleverancier in combinatie met de BlackEnergy-malware. [3] Volgens diverse onderzoekers is de BlackEnergy-malware niet de directe oorzaak van de stroomuitval en is het waarschijnlijker dat een handmatige (digitale) actie van een aanvaller hiertoe heeft geleid. [4] Sommige bronnen melden dat de aanvallers daarnaast gelijktijdig ook een telefonische Denial-of-Service-aanval hebben uitgevoerd waardoor de stroomproducent telefonisch niet bereikbaar was. [5][6] Na de berichtgeving over het incident in Oekraïne verschenen nog diverse andere meldingen over incidenten die hieraan gerelateerd zouden kunnen zijn. Zo zou BlackEnergy recent ook zijn ingezet tegen een Oekraïense luchthaven, maar leidde dit niet tot schade. [7] Daarnaast lijkt een vermeende aanval op het energienetwerk in Israël uiteindelijk "niet meer" te zijn dan een succesvolle ransomware-aanval op de toezichthouder in dat land. [8]

11

[redacted]

11

Het NCSC heeft recent een geactualiseerde factsheet gepubliceerd die beschrijft welke risico's het koppelen van ICS/SCADA-systemen aan internet met zich meebrengt en welke maatregelen organisaties kunnen treffen om deze systemen beter te beveiligen.

11

[redacted]

A

[redacted]

A

[redacted]


A
A
A
A
A
A

versie 1.0 | 4 mei 2016

TLP: GREEN

Nationaal Cyber Security Centrum
Ministerie van Veiligheid en Justitie

NCSC Maandmonitor

April 2016

A

[redacted]

A

[redacted]

A

[redacted]

A

[redacted]

Oude wormen in een Duitse kerncentrale

Bij een kerncentrale in Gundremmingen, Duitsland, is malware aangetroffen op een computer die de laadmachine voor brandstofelementen aanstuurt. De schadelijke software werd ontdekt tijdens voorbereidingen op een revisie van een onderdeel van de centrale. [7]

Reuters meldt dat de aangetroffen malware o.a. "W32.Ramnit" en "Conficker" betreft. [8] De primaire functionaliteit van de W32.Ramnit worm is het stelen van informatie. Daarnaast biedt de worm ook de mogelijkheid om toegang te verkrijgen tot de bestanden op een geïnfecteerd systeem. Conficker is een malware uit 2008 dat computersystemen toevoegt aan een botnet. De malwarebesmetting zou geen gevaar voor het personeel of de bevolking hebben opgeleverd, omdat de gevoelige systemen van de centrale niet op het internet zijn aangesloten.

Na de ontdekking zijn alle andere computersystemen in de centrale onderzocht. Hier werd geen malware op aangetroffen. [9]

Op dit moment wordt onderzocht hoe de besmetting plaats heeft gevonden. Er zou ook malware zijn aangetroffen op verwijderbare opslagmedia, voornamelijk USB sticks, in de kantooromgeving (gescheiden van de procesomgeving). [10] Vooralsnog wordt er vanuit gegaan dat het gaat om een onopzettelijke besmetting via een USB-stick. De aangetroffen malware komt veel voor op privé- en bedrijfscomputers en de kans zou volgens diverse media klein zijn dat het om een gerichte aanval gaat. [11] [12]

11

[redacted]

11

A

A

A

A

A

A

Nationaal Cyber Security Centrum
Ministerie van Veiligheid en Justitie

NCSC Maandmonitor – juni 2017

A [redacted]

A [redacted]

A [redacted]

Industroyer/CrashOverride

Door een cyberaanval op het energienetwerk in Oekraïne in december 2016 kwamen 225.000 mensen enkele uren zonder stroom te zitten. [4] De malware die hiervoor mogelijk verantwoordelijk was, is in staat met industriële controlesystemen (ICS) te communiceren die voor de aansturing van energienetwerken worden gebruikt. Dit blijkt uit het onderzoeksrapport dat beveiligingsbedrijf ESET heeft uitgebracht. [5] De malware, Industroyer (ook wel CrashOverride genoemd), is toepasbaar in andere industrieën, aangezien deze eveneens in staat is met gestandaardiseerde protocollen te communiceren, die in het overgrote deel van ICS worden gebruikt. Voordat de malware kan worden ingezet, is echter wel toegang tot het netwerk van het doelwit noodzakelijk. Het rapport bevat geen informatie over hoe de aanvallers het netwerk zijn binnengekomen.

11 [redacted]

A [redacted]

A [redacted]

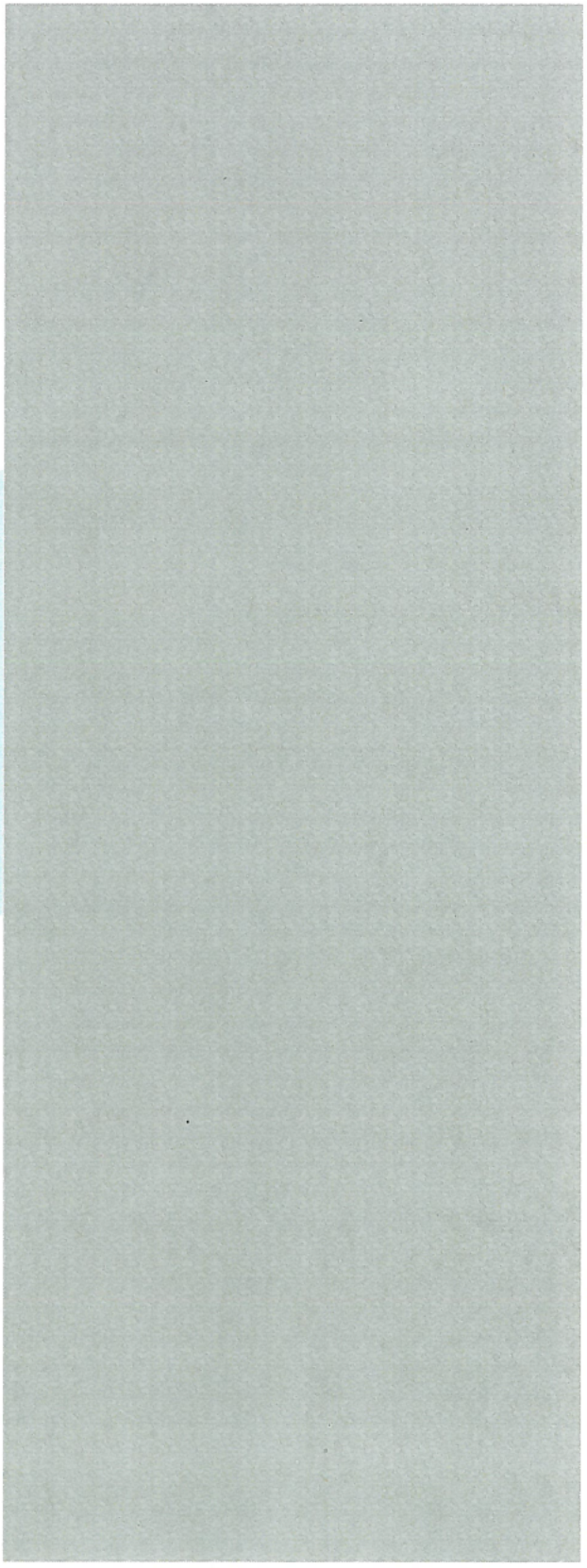
TLP:GREEN

Nationaal Cyber Security Centrum
Ministerie van Veiligheid en Justitie

NCSC Maandmonitor – januari 2018

A

A

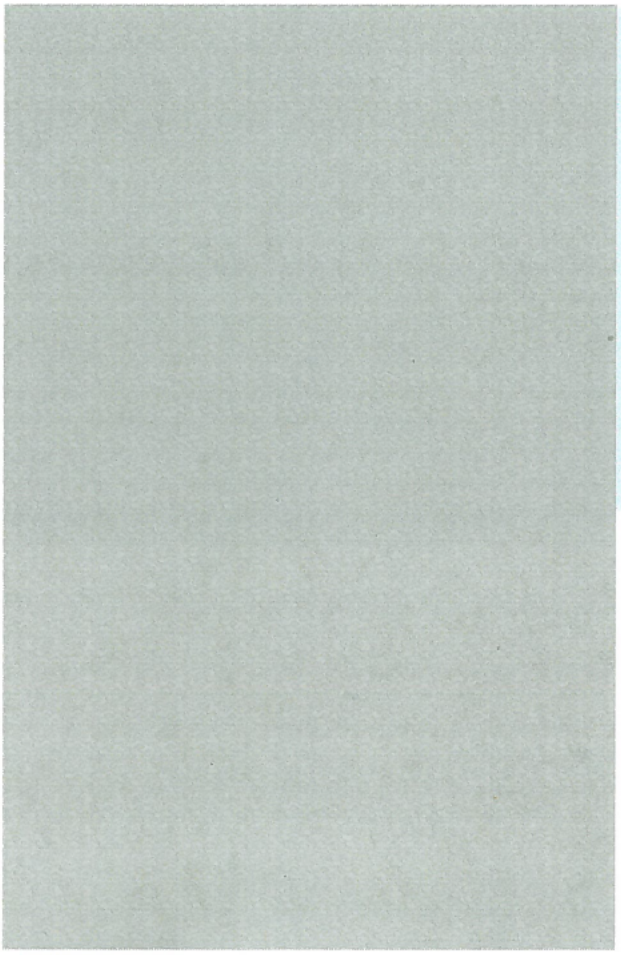


TRITON/TRISIS-malware

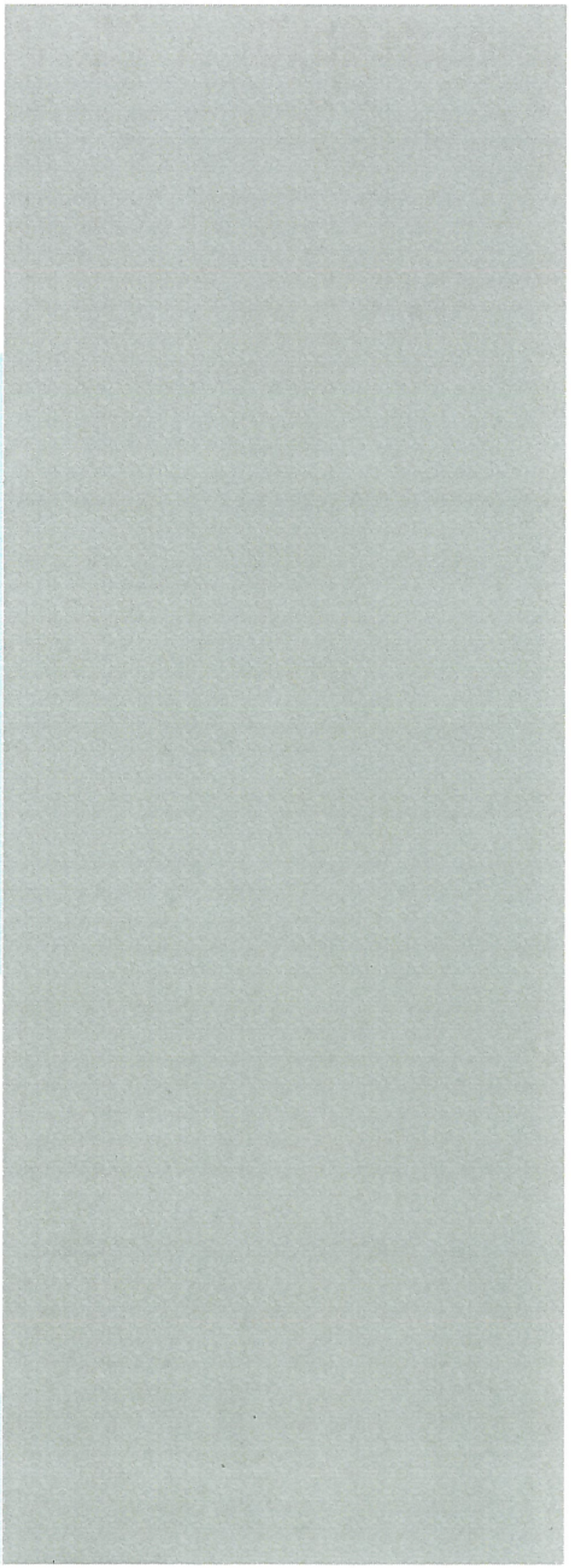
FireEye, Symantec, Dragos en Schneider Electric melden dat er in ieder geval sinds september malware is ontdekt die Schneider Electric Triconex Safety Instrumented Systems kan herprogrammeren. [1] [2] [3] Dergelijke systemen zijn er als back-up om de veiligheid van bijvoorbeeld chemische of nucleaire industriële processen te garanderen, indien er problemen zijn met het reguliere controlesysteem. Deze TRITON/TRISIS-malware maakt misbruik van een zeroday-kwetsbaarheid, van waaruit er een remote access trojan (RAT) geïnstalleerd wordt. Dit constateert Schneider Electric na onderzoek bij een klant waar de malware aangetroffen is.

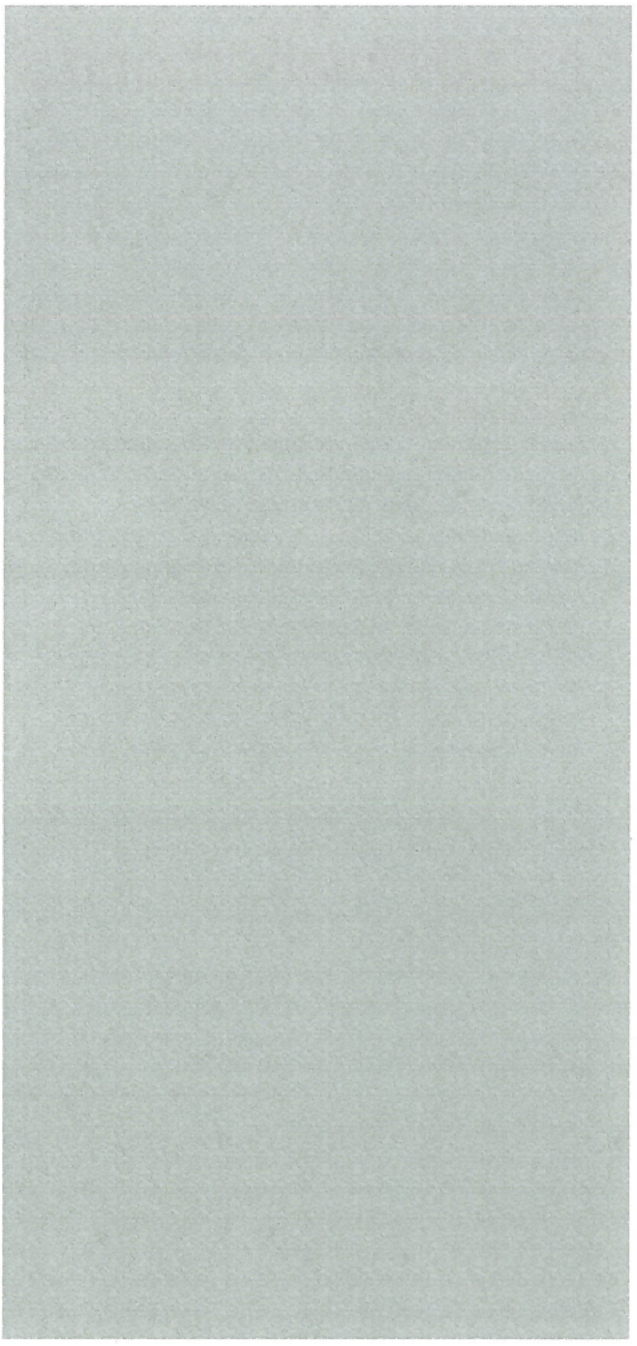
11

A



A





A

Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

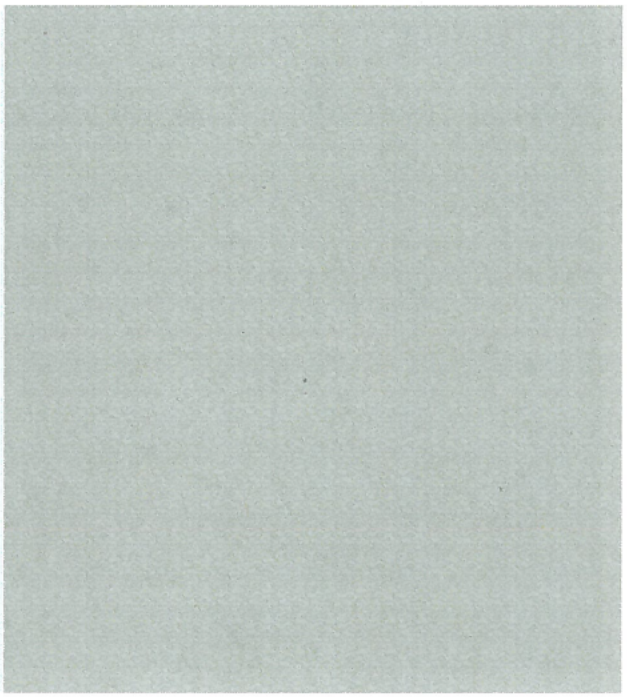
NCSC Maandmonitor – maart 2018

A

Mislukte sabotage van petrochemische fabriek in Saoudi-Arabië

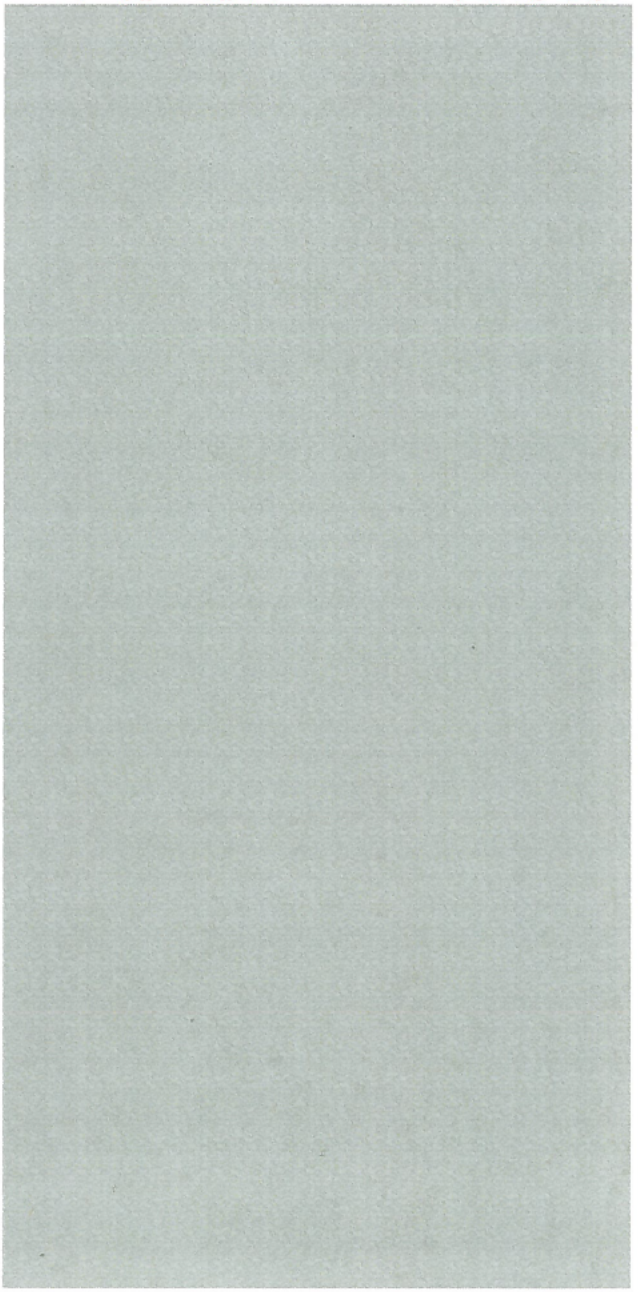
In december vorig jaar werd malware ontdekt die Schneider Electric Triconex Safety Instrumented Systems (SIS) kan herprogrammeren. Deze safety controllers worden ingezet als back-up voor de veiligheid van bijvoorbeeld chemische of nucleaire industriële processen, ook als er problemen zijn met het reguliere controlesysteem. Deze Triconex-systemen worden wereldwijd in duizenden fabrieken gebruikt. Zie ook de maandmonitor van januari 2018 waarin de malware, met de namen TRITON en TRISIS, al werd beschreven.
Deze maand was er hernieuwde aandacht voor deze malware. De New York Times berichtte dat de malware zou zijn ingezet voor een sabotagepoging van een petrochemische fabriek in Saoedi-Arabië. Volgens de New York Times zou de malware als doel hebben de operatie te saboteren en een explosie te veroorzaken. Een bug in de malware lijkt een explosie te hebben voorkomen. Vanwege de geavanceerdheid van de aanval wordt deze door onderzoekers in verband gebracht met een statelijke actor. [1]

11

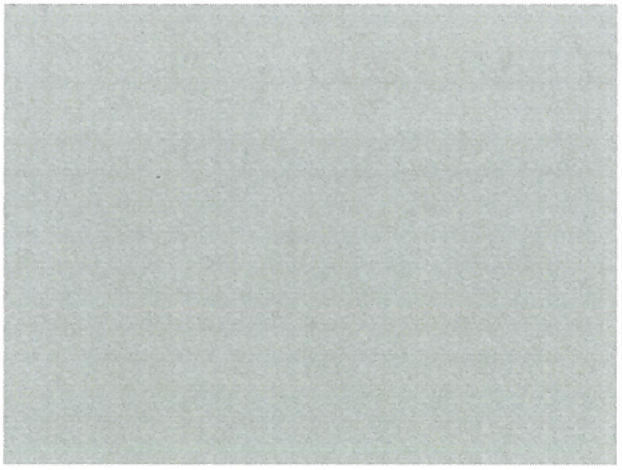


A

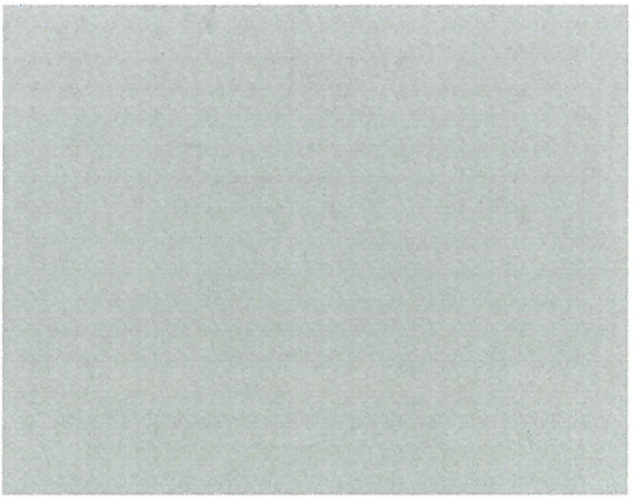
A



A

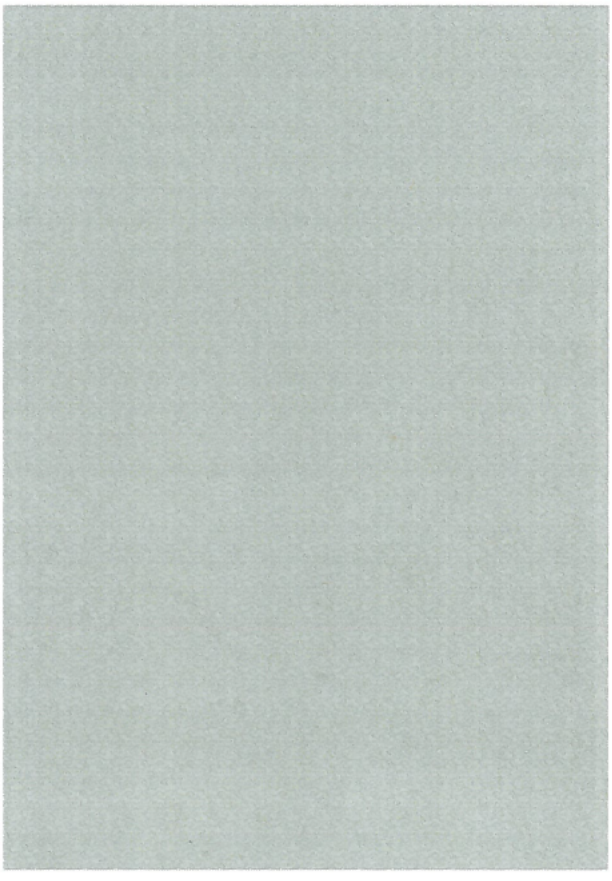


A

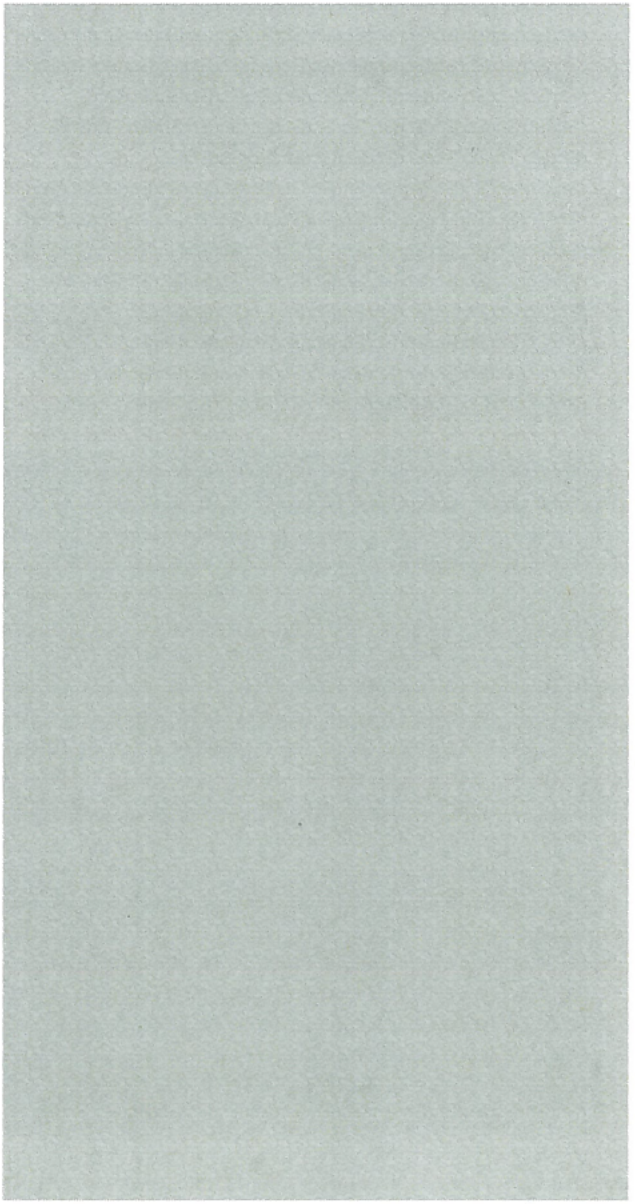


A

A



A



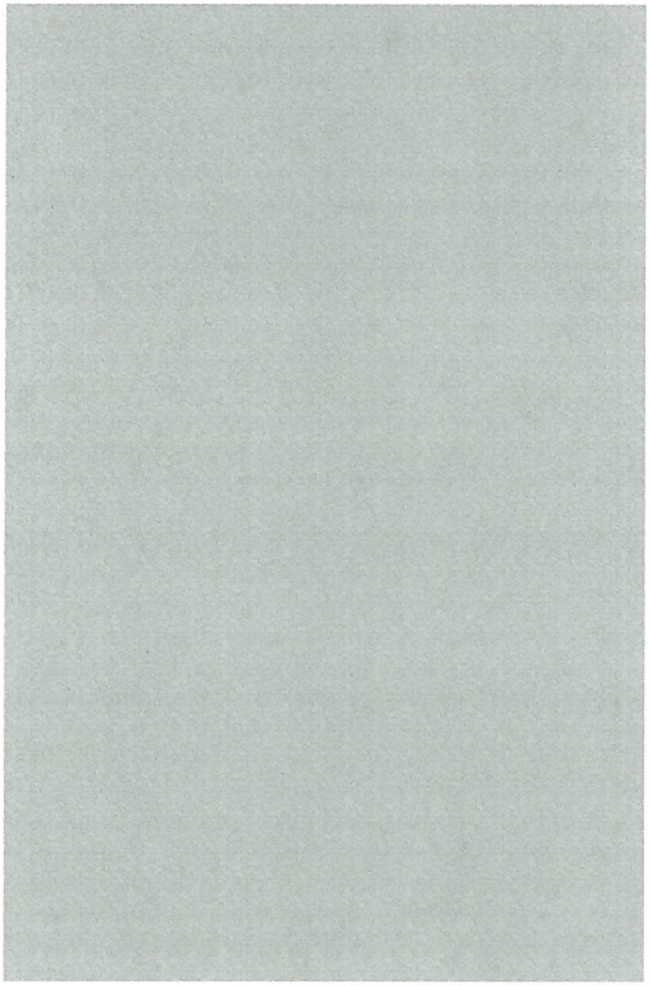
TLP:GREEN

Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC Maandmonitor – oktober 2018

A

A

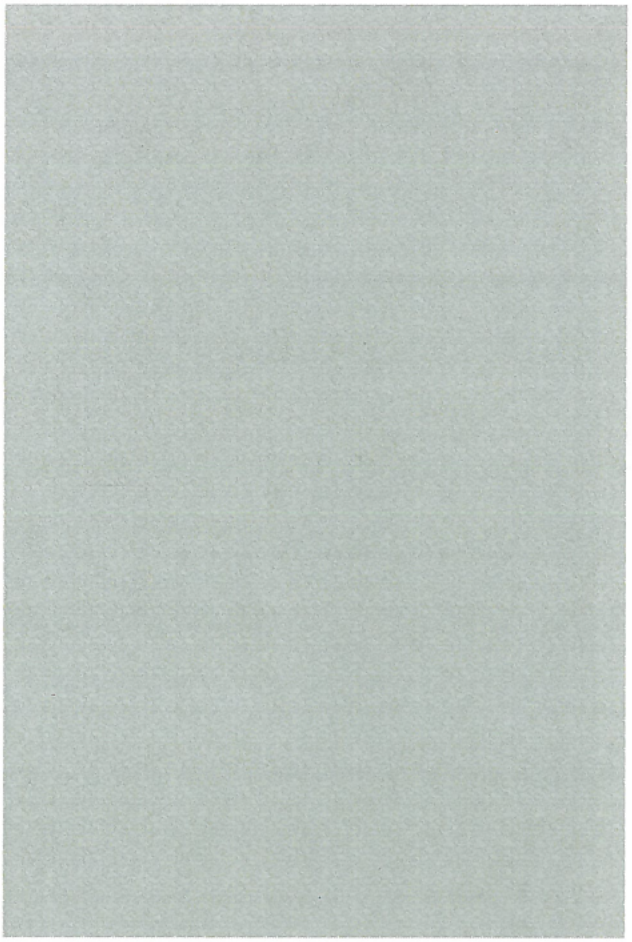


Aanvallen van GreyEnergy op Europese vitale infrastructuren

Een ICT-beveiligingsbedrijf heeft een onderzoeksrapport uitgebracht over de nieuwe hackergroep 'GreyEnergy'. [9] Het onderzoeksrapport schetst onder andere overeenkomsten in gebruikte tools, tactieken en procedures met de digitale aanvallen door BlackEnergy, die in het najaar van 2015 en 2016 voor elektriciteitsproblemen zorgden in Oekraïne. GreyEnergy heeft digitale aanvallen uitgevoerd op organisaties die deel uitmaken van de vitale infrastructuur, en dan met name de energiesector. [10] De aanvallen zijn vooralsnog uitgevoerd op doelwitten in Oekraïne en Polen, mogelijk met het toekomstige doel om vitale infrastructuren in andere landen te saboteren.

GreyEnergy wordt in het rapport benoemd als de opvolger van BlackEnergy. GreyEnergy gebruikt een overeenkomstige malwaretoolkit van BlackEnergy, alleen deze variant blijft langer onopgemerkt in het netwerk. Daarnaast verwijdert het de sporen van de malwarecomponenten, waardoor detectie lastiger wordt.

11



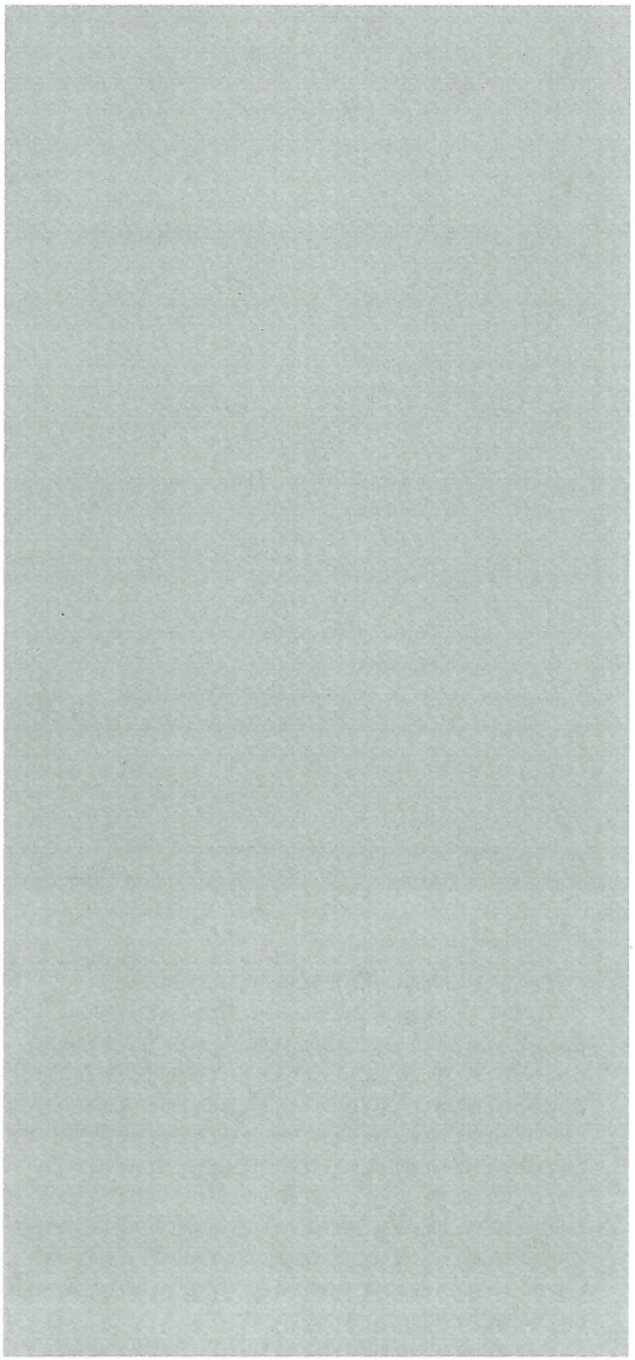
A

TRITON/TRISIS-malware gelinkt aan Russisch onderzoeksinstituut

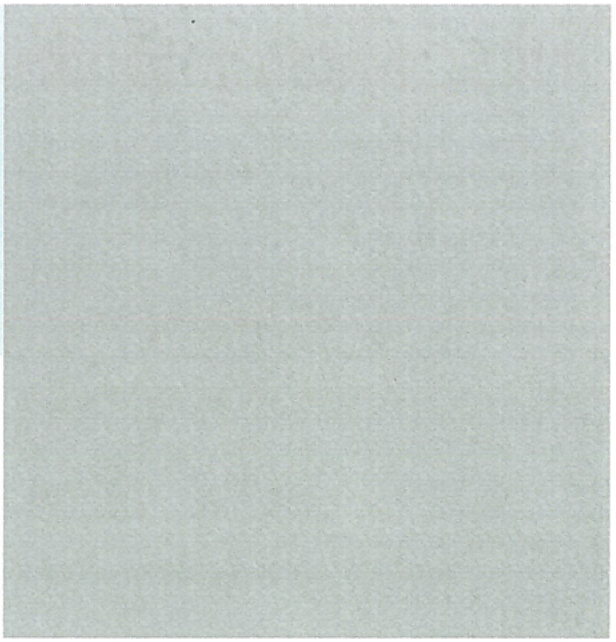
Al in eerdere edities van de maandmonitor 2018 kwam TRITON/TRITIS aan bod. Destijds betrof het een Saoedische petrochemische fabriek die besmet was met de TRITON/TRISIS-malware. [16] Deze malware maakt het mogelijk om de Safety Instrumented-Systems (SIS) te herprogrammeren. Een SIS wordt gebruikt als een back-up controlesysteem bij voornamelijk nucleaire en chemische industriële processen. Door het herprogrammeren van deze systemen is de aanvaller in staat het veiligheidsmechanisme uit te schakelen wat tot fysieke gevolgen kan leiden. [17] Het bedrijf dat verantwoordelijk is voor de firmware waarin de kwetsbaarheid zich bevond, heeft hier eerder dit jaar patches voor uitgebracht.
Nu is er opnieuw aandacht voor de TRITON/TRISIS-malware nadat uit onderzoek van een ICT-beveiligingsbedrijf zou zijn

gebleken dat een Russisch onderzoeksinstituut mogelijk betrokken is bij de uitvoering van de aanval. [18] Het genoemde instituut doet onder andere onderzoek naar toegepaste mechanica en nanotechnologie en het vervaardigen van chemieproducten. Het gebruikte cyrillisch schrift, de tijdzone waarin gewerkt werd, het IP-adres waarvandaan de malafide activiteiten werden uitgevoerd en een aantal andere indicatoren hebben de beveiligingsonderzoekers doen overtuigen dat het Russische onderzoeksinstituut verantwoordelijk gehouden kan worden voor de aanval.

11



A



A